



**IT Security Procedural Guide:
Audit and Accountability (AU)
CIO-IT Security-01-08**

Revision 5

November 3, 2017

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 2 – January 29, 2008				
1	Scott/Heard	Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1B requirements.	Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1B requirements.	Various
2	Scott/Heard	Changes throughout the document to correspond with revisions made to CIO-IT Security-01-09, CIO-IT Security-01-03 and CIO-IT Security-01-04.	Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents	Various
3	Hummel/Windelberg	Changes throughout the document to correspond with update of the current version of GSA CIO P 2100 and other updates	Update to the most current version of GSA CIO P 2100 and provide more detailed guidance on implementing policy.	Various
Revision 3 – June 30, 2010				
1	Berlas/Cook	Changes throughout the document to correspond with update of the current version of GSA CIO P 2100 and NIST 800-53 rev3.	Update to the most current version of GSA CIO P 2100 and provide more detailed guidance on implementing policy.	Various
Revision 4 – March 22, 2017				
1	Wilson/Yardley/Klemens	Changes throughout the document to correspond with update of the current version of NIST 800-53 Rev4.	Update to NIST 800-53, Rev 4 and correlate with GSA Guidance on parameters and implementation.	Various
Revision 5 – November 3, 2017				
1	Feliksa/Heffron/Klemens	Updated format and NIST SP 800-53 control parameters, and incorporated current Federal regulations and guidance.	Incorporate most current Federal regulations, NIST guidance, and GSA requirements.	Various

APPROVAL

IT Security Procedural Guide: Audit and Accountability (AU), CIO-IT Security-01-08, Revision 5 is hereby approved for distribution.

11/9/2017

X Kurt Garbars

Kurt Garbars

CISO

Signed by: KURT GARBARS

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

1	Introduction	1
1.1	Purpose.....	3
1.2	Scope	3
1.3	Policy.....	3
1.4	References	4
2	Roles and Responsibilities.....	4
2.1	The Chief Information Officer (CIO).....	4
2.2	The Chief Information Security Officer (CISO).....	5
2.3	Authorizing Official (AO).....	5
2.4	Information Systems Security Manager (ISSM).....	5
2.5	Information System Security Officer (ISSO).....	5
2.6	System Owner.....	6
2.7	Data Owners	6
2.8	System/Network Administrators.....	6
3	GSA Implementation Guidance for AU Controls	7
3.1	AU-1 Audit and Accountability Policy and Procedures.....	7
3.2	AU-2 Auditable Events.....	8
3.3	AU-3 Content of Audit Records	10
3.4	AU-4 Audit Storage Capacity	11
3.5	AU-5 Response to Audit Processing Failures	12
3.6	AU-6 Audit Review, Analysis, and Reporting	13
3.7	AU-7 Audit Reduction and Report Generation	14
3.8	AU-8 Time Stamps	16
3.9	AU-9 Protection of Audit Information	16
3.10	AU-10 Non-Repudiation	18
3.11	AU-11 Audit Record Retention	18
3.12	AU-12 Audit Generation	19
4	Summary.....	20

Table of Figures and Tables

Table 1-1: NIST SP 800-53 Control to CSF Mapping.....	2
--	----------

1 Introduction

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. When complemented with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including but not limited to: (1) establishing individual accountability; (2) detecting security violations and intrusions; (3) identifying flaws in systems and applications; (4) performing problem analysis; and (5) assisting in incident reconstruction.

When auditing is not implemented, is improperly configured, and/or the resultant audit logs are not regularly reviewed the following outcomes may occur in the event of a system compromise.

- an incident may go undetected
- an attacker may hide their location, malicious software, and their activities on the compromised host
- user accountability for actions may be unsupported
- system changes may not be noticed

If a compromise is detected, without protected and complete logging records, those charged with the security responsibility for the system are blind to the details of the attack. The attack may go unnoticed, with attackers sometimes controlling compromised machines for months or years without anyone in the organization knowing, even though the evidence of the attack has been recorded in unexamined log files. Audit records may be the only evidence of a successful attack.

Audit logging cannot be just for compliance purposes. They must be generated for the purpose of proactive review, including real-time analysis, ongoing periodic reviews, and to establish what occurred after an event. Reviewers should know what to look for to effectively spot unusual activity, and understand the normal activity for the systems under their purview.

Every General Services Administration (GSA) Information Technology (IT) system must follow the Audit and Accountability (AU) practices identified in this guide. Any deviations from the security requirements established in [GSA Order CIO 2100.1](#), “*GSA Information Technology (IT) Security Policy*” must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the [Security Deviation Request Google Form](#).

Executive Order (EO), [EO 13800](#), “*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*” requires all agencies to use “[The Framework for Improving Critical Infrastructure Cybersecurity](#)” (the Framework) developed by the National Institute of Standards and Technology (NIST) or any successor document to

manage the agency’s cybersecurity risk.” This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. The CSF complements, and does not replace, an organization’s risk management process and cybersecurity program. GSA uses NIST’s Risk Management Framework from [NIST SP 800-37, Revision 1](#), “*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.” Table 1-1 provides how the NIST SP 800-53 security controls in this guide are aligned with the CSF Category Unique Identifiers.

Table 1-1: NIST SP 800-53 Control to CSF Mapping

NIST SP 800-53 Security Controls	CSF Category Unique Identifier Codes
AU-1	ID.GV-1, ID.GV-3, PR.PT-1
AU-2	PR.PT-1
AU-3	PR.PT-1
AU-4	PR.DS-4, PR.PT-1
AU-5	PR.PT-1
AU-6	PR.PT-1
AU-7	PR.PT-1
AU-8	PR.PT-1
AU-9	PR.PT-1
AU-10	PR.PT-1
AU-11	PR.PT-1
AU-12	PR.PT-1, DE.CM-1, DE.CM-3, DE.CM-7

The CSF category descriptions aligned with NIST’s AU controls are provided below.

ID.GV: Identify-Governance

- ID.GV-1: Organizational information security policy is established.
- ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

PR.DS: Protect-Data Security

- PR.DS-4: Adequate capacity to ensure availability is maintained.

PR.PT: Protect-Protective Technology

- PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

DE.CM: Detect-Security Continuous Monitoring

- DE.CM-1: The network is monitored to detect potential cybersecurity event.
- DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
- DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.

The audit and accountability principles and practices described in this guide are based on guidance from the NIST including NIST SP 800-53, Revision 4, “*Security and Privacy Controls for Federal Information Systems and Organizations*.” This guide provides an overview of audit and accountability, roles and responsibilities, NIST SP 800-53 audit and accountability requirements per [Federal Information Processing Standard \(FIPS\) Publication \(PUB\) 199](#), “*Standards for Security Categorization of Federal Information and Information Systems*” security categorization level, and procedures for implementing these requirements.

1.1 Purpose

The purpose of this guide is to provide guidance for the AU security controls identified in NIST SP 800-53 and auditing and accountability requirements specified in CIO 2100.1. The guide provides GSA Federal employees, contractors with significant security responsibilities (as identified in CIO 2100.1), and other IT personnel involved in implementing auditing and monitoring, the specific procedures they are to follow for implementing AU features and functions for systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in audit and accountability of GSA information systems and data.

1.3 Policy

Auditing and accountability is covered in Chapter 5, paragraph 2 of CIO 2100.1 as stated in the following paragraphs:

c. Audit Records.

- (1) Security-activity auditing capabilities must be employed on all GSA information systems using IT Security Procedural Guide: Auditing & Monitoring, CIO-IT Security-01-08 and NIST SP 800-37 R1 as guides.*
- (2) Audit records must be regularly reviewed/analyzed for indications of inappropriate or unusual activity. Suspicious activity or suspected violations must be investigated. Any findings must be reported to appropriate officials IAW IT Security Procedural Guide: Incident Response, OCIO-IT Security-01-02.*
- (3) Intrusion detection systems must be implemented as deemed appropriate by the AO.*
- (4) Information systems must alert appropriate organizational officials in the event of an audit processing failure and take one of the following additional actions: shut down information system, overwrite oldest audit records, or stop generating audit records.*
- (5) Information systems must produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.*
- (6) Audit log data must be archived for a period of not less than 180 days.*

(7) Systems that contain permanent electronic records must be maintained in an electronic format by 12/31/2019.

(8) All permanent and temporary e-mail records must be accessible electronically in an electronic format.

1.4 References

- [EO 13800](#), "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- [Cybersecurity Framework](#), "Framework for Improving Critical Infrastructure Cybersecurity"
- [GSA Order CIO 2100.1](#), "GSA Information Technology (IT) Security Policy"
- [FIPS PUB 199](#), "Standards for Security Categorization of Federal Information and Information Systems"
- [NIST SP 800-37, Revision 1](#), "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- [NIST SP 800-53, Revision 4](#), "Security and Privacy Controls for Federal Information Systems and Organizations"
- [CIO-IT Security-01-02](#), "Incident Response (IR)"
- [CIO-IT Security-07-35](#), "Web Application Security"
- [GSA ISPP](#), "Information Security Program Plan"
- [GSA CTW](#), "Control Tailoring Workbook"

2 Roles and Responsibilities

There are many roles associated with implementing effective auditing and logging, and reviews of the records produced. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Throughout this guide, specific processes and procedures for implementing auditing and accountability are described.

2.1 The Chief Information Officer (CIO)

Responsibilities include the following:

- Developing and maintaining an agency-wide GSA IT Security Program.
- Ensuring the agency effectively implements and maintains information security policies and guidelines.
- Providing management processes to enable the AO to implement the components of the IT Security Program for which they are responsible.

2.2 The Chief Information Security Officer (CISO)

Responsibilities include the following:

- Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies.
- Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with CIO 2100.1.
- Developing and implementing procedures for detecting, reporting, and responding to security incidents.

2.3 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required AU controls in accordance with GSA and Federal policies and requirements.
- Accepting the risk of operating GSA information systems under their purview where AU controls have not been fully implemented.
- Ensuring a plan of action and milestones (POA&M) item is established and managed to address AU controls that are not fully implemented.

2.4 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Monitoring and supporting the resolution of POA&Ms to mitigate system vulnerabilities regarding AU controls for all systems under their purview.
 - Ensuring POA&Ms are developed and documented within the GSA POA&M Team Drives.
 - Ensuring ISSOs and System Owners are maintaining POA&Ms for their systems, including taking remediation actions according to the scheduled milestones.
- Coordinating with ISSOs to establish and manage auditing and monitoring procedures (e.g., reviewing and coordinating the reporting of security alerts, performance of audit log reviews, supporting the use of auditing/logging as part of security incident investigations and reports, etc.)

2.5 Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary AU security controls are in place and operating as intended.
- Developing POA&Ms regarding AU controls for all systems under their purview.
- Reviewing system security audit trails and system security documentation to ensure security measures are implemented effectively.
- Coordinating the establishment of auditing and monitoring procedures.

- Managing auditing and monitoring processes.

2.6 System Owner

Responsibilities include the following:

- Ensuring audit records meet the base AU security control requirements.
- Ensuring audit record formats can be processed by the Enterprise Logging Platform.
- Ensuring necessary AU security controls are in place and operating as intended.
- Obtaining and allocating the security resources for their respective systems.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms regarding AU controls for their respective systems.
- Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.
- Working with Data Owners to ensure that log data is archived for a period of not less than 180 days.
- Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities.
- Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

2.7 Data Owners

Responsibilities include the following:

- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of AU control requirements.
- Working with the System Owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.
- Working with the System Owner to ensure that log data is archived for a period of not less than 180 days.
- Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities.
- Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

2.8 System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate AU security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- Working with the Custodian/ISSO to ensure appropriate technical AU security requirements are implemented.

3 GSA Implementation Guidance for AU Controls

The GSA-defined parameter settings included in the control requirements are offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements in this guide apply to GSA Federal employees and contractors who are involved in audit and accountability of GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions/requirements for contractor systems will be included in the “Additional Contractor System Considerations” portion of each control section. If “None” is listed for “Additional Contractor System Considerations” it means there are no additional requirements, the system still needs to comply with the overall implementation guidance.

AU-1, Audit and Accountability Policy and Procedures, has been identified as a Common Control for all GSA/internally operated systems by GSA and as a Hybrid Control for contractor systems. The AU-2 to AU-12 controls, when included in a system’s control set, either are provided as a Common Control by a General Support System, a system specific control by the system, or as a Hybrid Control with shared responsibilities for control implementation. GSA’s [“Information Security Program Plan”](#) describes GSA’s enterprise-wide inheritable common and hybrid controls.

3.1 AU-1 Audit and Accountability Policy and Procedures

Control: The organization:

- a. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians*]:
 1. An audit and accountability policy that addresses purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
- b. Reviews and updates the current:
 1. Audit and accountability policy [*biennially*]; and
 2. Audit and accountability procedures [*biennially*].

GSA Implementation Guidance: Control AU-1 is applicable at all FIPS 199 levels.

CIO 2100.1 describes the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements for GSA’s security program, including AU controls. Chapter 5, paragraph 2c, Audit records, of CIO 2100.1 identifies specific audit requirements for all GSA systems.

Audit and accountability procedures are documented in this guide. The procedures facilitate the implementation of the audit policy and associated controls.

AU policy requirements, as listed in CIO 2100.1, and procedures as provided in this procedural guide, are reviewed and updated biennially and are disseminated via the [GSA IT Security](#) InSite page.

Additional Contractor System Considerations:

Vendor/Contractor systems may defer to GSA policy as identified above and in CIO 2100.1 or implement their own audit and accountability policies and procedures which comply with GSA's requirements with the approval of the AO.

3.2 AU-2 Auditable Events

Control: The organization:

- a. Determines that the information system is capable of auditing the following events: *[successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events; Web applications should log all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; for technologies with limited auditing features, the capabilities will be recommended by the GSA S/SO or Contractor, based on an industry source such as vendor guidance or Center for Internet Security benchmark, and approved by the GSA AO];*
- b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
- c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
- d. Determines that the following events are to be audited within the information system: *[audit configuration requirements as documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log; for technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA S/SO or Contractor and approved by the GSA AO].*

Control Enhancements:

- (3) Audit Events | Reviews and Updates. The organization reviews and updates the audited events *[annually or whenever there is a change in the system's threat environment as communicated by the GSA S/SO AO or the GSA OCISO].*

GSA Implementation Guidance: Control AU-2 is applicable at all FIPS 199 levels. Enhancement AU-2(3) is applicable at FIPS 199 Moderate and High levels.

Common Control Implementation:

The GSA OCISO Security Operations (ISO) division provides an Enterprise Logging Platform which may be used by the system owner to forward all auditable Operating System events. These events will be retained by ISO Security Operations for a period of time which meets or exceeds GSA records retention policies. These events may be requested for review of system performance, analysis, or incident response, but are not reviewed on a regular basis.

All auditable events for web applications, database systems, non-system utilities, and Operating Systems not enrolled in the Enterprise Logging Platform will be retained by the system owner for a period of time which meets or exceeds GSA records retention policies.

The ISO division uses host-based intrusion detection (HIDS) systems in order to correlate Operating System auditable events which may trigger alerts on security events which are further analyzed and correlated with other security systems in the Enterprise Logging Platform. FISMA system owners may request HIDS implementation on an individual Operating System, and, if supported, HIDS security events will be forwarded to the Enterprise Logging Platform. These security events are maintained, managed, and correlated by ISO Security Operations and reviewed in the Enterprise Logging Platform by the ISO Security Operations Center (SOC).

Additional guidance for logging of auditable events and correlation of security alerts can be found in the [GSA Logging and Audit Compliance Guidance](#) document for meeting NIST SP 800-53 AU controls.

For enhancement AU-2(3), GSA reviews and updates the audited events annually or whenever there is a change in the system's threat environment as communicated by the GSA S/SO AO or the GSA OCISO.

System Specific Expectations for GSA/Internally Operated Systems:

ISSOs retain the responsibility of verifying that logging is correctly configured and processed. Auditable events that are not forwarded to the Enterprise Logging Platform will need to be managed by the ISSO on the system where they are stored (e.g., locally on the server or a separate log system).

For enhancement AU-2(3), when auditable events are managed locally on the server or a separate log server, audited system events must be reviewed and updated by the ISSO/system owner annually or whenever there is a change in the system's threat environment.

Note: A summary of the GSA defined audit policy settings can be found within GSA system hardening guides on the GSA [IT Security Technical Guides and Standards](#) InSite page. These technical guides and associated benchmarks provide detailed information on configuring security auditing for each of the common Operating Systems used within GSA, as well as recommended policy settings for web and database applications.

Additional Contractor System Considerations: None.

3.3 AU-3 Content of Audit Records

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Control Enhancements:

- (1) Content of Audit Records | Additional Audit Information. The information system generates audit records containing the following additional information:
 - i. *Session, connection, transaction, or activity duration.*
 - ii. *For client-server transactions, the number of bytes received and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry.*
 - iii. *For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier or browser characteristics (e.g. a 'User-Agent' string).*
 - iv. *Details regarding the event 'type': the type of method (for HTTP: GET/POST/HEAD, etc.) or action (Database INSERT, UPDATE, DELETE).*
 - v. *Characteristics that describe or identify the object or resource being acted upon.*
 - vi. *Additional informational messages to diagnose or identify the event].*
- (2) Content of Audit Records | Centralized Management of Planned Audit Record Content. The information system provides centralized management and configuration of the content to be captured in audit records generated by *[GSA S/SO or Contractor recommended information system components to be approved by the GSA AO]*.

GSA Implementation Guidance: Control AU-3 is applicable at all FIPS 199 levels. Enhancement AU-3(1) is applicable at the FIPS 199 Moderate and High levels. Enhancement AU-3 (2) is also applicable at the FIPS 199 High level.

Common Control Implementation:

Audit records that are forwarded to the Enterprise Logging Platform must be formatted as such that they can be properly processed by the Enterprise Logging Platform, e.g., in a standard syslog format or the Common Event Format. The Enterprise Logging Platform may have different requirements depending on the data source vendor, version, etc., to ensure it meets the base requirements. Generally, if an audit record can be parsed by the Enterprise Logging Platform, it will meet the base requirements.

For enhancement AU-3(1) parameters i and ii, only traffic that traverses the GSA perimeter firewall or Intrusion Prevention Systems (IPS) devices is captured by the Enterprise Logging Platform. For AU-3(1) parameters iii, iv, v, and vi, only HTTP traffic and HTTPS traffic (when the

HTTPS private key is available for session decryption) where the traffic traverses the perimeter firewalls or IPSs is also captured by the Enterprise Logging Platform.

For enhancement AU-3(2), the GSA OCISO ISO division will work with the system owner to determine the appropriate information system components.

System Specific Expectations for GSA/Internally Operated Systems:

The FISMA system owner is responsible for ensuring that audit records meet the base requirement and that the formatting can be processed by the Enterprise Logging Platform. This could involve working with the vendor or OCISO ISO division to fund creation of, or create log parsers; or alternatively work with the vendor of the audit record source to ensure the records are formatted in a parsable common event format.

For enhancement AU-3(1), the FISMA system owner is responsible for ensuring that the system is configured and meets the requirements. Typically, this means that a web server has W3C extended logging enabled and includes the required fields, including any significant GET/PUT parameters used in the application. For Enhancement AU-3(1), PII data and sensitive data such as credit card data shall NOT be stored in the logs, unless they are obfuscated.

For enhancement AU-3(2), the GSA OCISO ISO division will work with the system owner to determine the appropriate information system components.

Note: The system owner may choose to manage and configure the content to be captured locally unless enhancement AU-3(2) is required. The system owner may also elect to coordinate with the GSA OCISO ISO division to manage and configure content to be captured, regardless of FIPS 199 security categorization.

Additional Contractor System Considerations: None.

3.4 AU-4 Audit Storage Capacity

Control: The organization allocates audit record storage capacity in accordance with [GSA policies and guidance: audit log sizes are documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides) available on the IT Security Technical Guides and Standards webpage (<https://insite.gsa.gov/portal/content/627210>)].

GSA Implementation Guidance: Control AU-4 is applicable at all FIPS 199 levels.

Common Control Implementation:

Desktops and servers that are members of the GSA Active Directory are managed through group policy objects and will be automatically configured to follow the GSA auditing policy and hardening guides for OS audit records once they are joined to the enterprise domain. Current setting for Windows servers and desktops is 65538 kilobytes (KB) for the System Log and Application Log and 196608 KB for the Security Log.

For system logs that are forwarded to the Enterprise Logging Platform, the Enterprise Logging Platform storage will be configured with enough storage to store the logs for the duration of time specified in [Section 3.11](#), AU-11 Audit Record Retention, in raw or aggregated form.

System Specific Expectations for GSA/Internally Operated Systems:

System owners are responsible for ensuring that systems are configured consistent with the IT Security policy, including application and database logs.

Detailed technical guidance for configuring log storage size for each of the common Operating Systems used within GSA, as well as web and database applications may be obtained from the internal GSA audit policies and on the [IT Security Technical Guides and Standards](#) InSite page.

System owners should configure auditing, whenever possible, so that records cannot exceed storage capacity and potentially negatively impact the OS or application.

Additional Contractor System Considerations: None.

3.5 AU-5 Response to Audit Processing Failures

Control: The information system:

- a. Alerts [*the GSA ISO Division via the Enterprise Logging Platform for systems integrated with the Enterprise Logging Platform; Administrators (Application, System, Network, etc.) for systems not integrated with the Enterprise Logging Platform*)] in the event of an audit processing failure; and
- b. Takes the following additional actions: [*shut down information system, overwrite oldest audit records, or stop generating audit records*].

Control Enhancements:

- (1) Response to Audit Processing Failures | Audit Storage Capacity. The information system provides a warning to [*Administrators (Application, System, Network, etc.)*] within [*GSA S/SO or Contractor recommended time period as approved by the GSA AO*] when allocated audit record storage volume reaches [*GSA S/SO or Contractor recommended percentage as approved by the GSA AO*] of repository maximum audit record storage capacity.
- (2) Response to Audit Processing Failures | Real-Time Alerts. The information system provides an alert in [*GSA S/SO or Contractor recommended time period as approved by the GSA AO*] to [*the GSA ISO Division via the Enterprise Logging Platform for systems integrated with the Enterprise Logging Platform; Administrators (Application, System, Network, etc.) for systems not integrated with the Enterprise Logging Platform*] when the following audit failure events occur: [*GSA S/SO or Contractor recommended audit failure events requiring real-time alerts as approved by the GSA AO*].

GSA Implementation Guidance: Control AU-5 is applicable at all FIPS 199 levels. Enhancements AU-5(1) and (2) are applicable at the FIPS 199 High level.

Common Control Implementation:

Logging sources managed in the Enterprise Logging Platform may be configured to alert if auditing or event logging ceases for a system.

System Specific Expectations for GSA/Internally Operated Systems:

The system owner must define the action to be taken upon log failure and must coordinate any Enterprise Logging Platform alerting with the GSA OCISO ISO division. The System Owner should troubleshoot the cause of the logging failure and work with the GSA OCISO ISO division to restore logging to the Enterprise Logging Platform.

Additional Contractor System Considerations: None.

3.6 AU-6 Audit Review, Analysis, and Reporting

Control: The organization:

- a. Reviews and analyzes information system audit records [*daily when security related events are forwarded to the Enterprise Logging Platform for automated analysis and correlation; otherwise on a periodic basis (specific period recommended by the GSA S/SO or Contractor and approved by the GSA AO);*] for indications of [*GSA S/SO or Contractor recommended inappropriate or unusual activity as approved by the GSA AO*]; and
- b. Reports findings to [*Information System Security Manager, Information System Security Officer, System Owner (e.g., System Program Manager, System Project Manager), Custodians, as designated and approved by the GSA AO, via a dashboard when security related events are forwarded to the Enterprise Logging Platform; otherwise via manual reporting mechanisms*].

Control Enhancements:

- (1) Audit Review, Analysis, and Reporting | Process Integration. The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
- (3) Audit Review, Analysis, and Reporting | Correlate Audit Repositories. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
- (5) Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities. The organization integrates analysis of audit records with analysis of [*information system monitoring information; GSA S/SO or Contractor recommended data/information collected from other sources as approved by the GSA AO*] to further enhance the ability to identify inappropriate or unusual activity.
- (6) Audit Review, Analysis, and Reporting | Correlation with Physical Monitoring. The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

GSA Implementation Guidance: Control AU-6 is applicable at all FIPS 199 levels. Enhancements AU-6(1) and (3) are applicable at the FIPS 199 Moderate level. Enhancements AU-6(1), (3), (5) and (6) are applicable at the FIPS 199 High level.

Common Control Implementation:

Aggregated and correlated logs and security-related events within the Enterprise Logging Platform are reviewed by GSA OCISO ISO division for indications of compromise on business days. GSA OCISO ISO division will manually report indications of compromise if they are not presented on the Enterprise Logging Platform dashboard.

For enhancement AU-6 (1), as necessary, the GSA OCISO ISO division's analysis will support investigations and response to suspicious activities conducted by the GSA Incident Response Team, IAW GSA IT Procedural Guide: [CIO-IT Security-01-02](#), "Incident Response (IR)."

For enhancement AU-6 (3), the Enterprise Logging Platform correlates security-related records across different security components and logging sources across GSA to gain organization-wide situational awareness.

For enhancement AU-6(5) and (6), as requested the GSA OCISO ISO division will coordinate with the GSA Incident Response Team to integrate analysis from other sources while suspicious activities are investigated.

System Specific Expectations for GSA/Internally Operated Systems:

The system owner maintains the responsibility of reviewing information system logs on their systems for unusual activity on a periodic basis defined on a system by system basis, and should keep a log that such a review has taken place.

For enhancement AU-6 (1), system owners should ensure that their system is covered by the Enterprise Logging Platform. In consultation with the GSA OCISO ISO division, this may include ensuring that the appropriate encryption ciphers are implemented and that the private Secure Sockets Layer (SSL) key and certificate are provided to the GSA OCISO ISO division. These steps will allow for SSL inspection of website traffic by the GSA perimeter firewalls and that appropriate audit records relevant to the system are forwarded to the Enterprise Logging Platform.

For enhancement AU-6 (3), system owners must ensure that logs are forwarded to the Enterprise Logging Platform.

Additional Contractor System Considerations: None.

3.7 AU-7 Audit Reduction and Report Generation

Control: The information system provides an audit reduction and report generation capability that:

- a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
- b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

- (1) Audit Reduction and Report Generation | Automatic Processing. The information system provides the capability to process audit records for events of interest based on:
 - *Source IP*
 - *Destination IP*
 - *Account Names*
 - *Date and Time of Events*
 - *Event Type*].

GSA Implementation Guidance: Control AU-7 and enhancement AU-7(1) are applicable at the FIPS 199 Moderate and High levels.

Common Control Implementation:

The Enterprise Logging Platform supports retrievable records for audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and is configured to aggregate logs and can be configured to generate reports as required.

Given the high volume of audit records collected, records of a similar nature may be aggregated such that only a subset of the data is retained, such as time of first and last event, number of events, along with the associated and relevant data points, if the majority of the data is identical.

For enhancement AU-7 (1), the Enterprise Logging Platform can process logs that have been forwarded to it based on parameters that include source IP, destination IP, account names, time and date of events and event type.

System Specific Expectations for GSA/Internally Operated Systems:

Logs that are not maintained in the Enterprise Logging Platform must be maintained by appropriate tools that facilitate audit reduction and report generation that can be provided to the GSA Incident Response Team in a timely fashion and in accordance with the GSA incident response policy.

For Enhancement AU-7 (1), the system owner is responsible for having logs forwarded to the Enterprise Logging Platform, or for implementing tools that can process, search, correlate logs based on the specified parameters if the logs are not forwarded to the Enterprise Logging Platform.

Additional Contractor System Considerations: None.

3.8 AU-8 Time Stamps

Control: The information system:

- a. Uses internal system clocks to generate time stamps for audit records; and
- b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets *[GSA S/SO or Contractor recommended granularity of time measurement to be approved by the GSA AO]*.

Control Enhancements:

- (1) Time Stamps | Synchronization with Authoritative Time Source. The information system:
 - (a) Compares the internal information system clocks [*at least hourly (the Microsoft default is every 45 minutes)*] with [*the internal network's authoritative time source*]; and
 - (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than *[GSA S/SO or Contractor recommended time period as approved by the GSA AO]*.

GSA Implementation Guidance: Control AU-8 is applicable at all FIPS 199 levels. Enhancement AU-8(1) is applicable at the FIPS 199 Moderate and High levels.

Common Control Implementation:

The Enterprise Logging Platform maintains log events in UTC, it can receive logs in any time zone, and can display the log events in the users' local time zone.

The Enterprise Logging Platform is in sync with the GSA time servers at ntp.gsa.gov, which use General Packet Radio Services (GPRS) for time synchronization.

System Specific Expectations for GSA/Internally Operated Systems:

Audit event sources must be configured to synchronize with an authoritative time source that is in sync with the GSA, NIST, or the Cloud Service Provider's time servers, e.g., Amazon Web Services.

Additional Contractor System Considerations: None.

3.9 AU-9 Protection of Audit Information

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Control Enhancements:

- (2) Protection of Audit Information | Audit Backup on Separate Physical Systems/Components. The information system backs up audit records [*at least weekly, unless the data is being sent to a secondary system, e.g., the Enterprise Logging*

Platform. The CISO reserves the right to determine if backups of specific audit records are required or not] onto a physically different system or system component than the system or component being audited.

- (3) Protection of Audit Information | Cryptographic Protection. The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.
- (4) Protection of Audit Information | Access by Subset of Privileged Users. The organization authorizes access to management of audit functionality to only [*privileged users specifically authorized to perform audit management functions (i.e., specified administrators of applications, systems, networks, etc.)*].

Note: ISSOs, ISSMs, and System Owners (i.e., Program Managers, Project Managers) may be provided read access to audit data; however, they will not have access to audit management functions.

GSA Implementation Guidance: Control AU-9 is applicable at all FIPS 199 levels. Enhancement AU-9(4) is applicable at the FIPS 199 Moderate level. Enhancements AU-9(2), (3) and (4) are applicable at the FIPS 199 High level.

Common Control Implementation:

Access to events in the Enterprise Logging Platform is restricted to users authorized by the OCISO ISO Division and/or the system ISSO or ISSM. The system owner must restrict access to local audit records to authorized personnel as designated by the ISSO/ISSM.

For enhancement AU-9 (2), where possible, all audit records will be sent to the Enterprise Logging Platform to meet the retention requirement. Where access to the Enterprise Logging Platform is not possible, audit records will be backed up at least weekly but preferably daily. Where possible, backups will be sent to Network Attached Storage or another form of highly redundant storage

For enhancement AU-9 (3), audit records not sent to the Enterprise Logging Platform should be encrypted at rest using encrypted disk volumes. A means of ensuring the integrity of the audit records will be implemented by leveraging mechanisms such as cryptographic checksums.

For enhancement AU-9 (4), access to events in the Enterprise Logging Platform is restricted to users authorized by the OCISO ISO Division and/or the system ISSO or ISSM. The system owner must restrict access to the management of audit records on the local system to authorized personnel as designated by the ISSO/ISSM.

System Specific Expectations for GSA/Internally Operated Systems:

The system owner protects audit logs that are not forwarded to the Enterprise Logging Platform by restricting access to only authorized personnel as designated by the ISSO/ISSM.

For enhancement AU-9 (4), the system owner protects audit logs that are not forwarded to the Enterprise Logging Platform by restricting access to only authorized personnel as designated by the ISSO/ISSM.

Additional Contractor System Considerations: None.

3.10 AU-10 Non-Repudiation

Control: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed *[system specific actions, e.g., such as electronically signing a document, approving a request, or receiving a message]*.

GSA Implementation Guidance: Control AU-10 is applicable at the FIPS 199 High Level.

Common Control Implementation:

The System Owner is responsible for ensuring that logging and audit settings are configured per GSA OCISO Security Engineering division's Technical Guides and Standards. This ensures an audit trail for non-repudiation purposes.

System Specific Expectations for GSA/Internally Operated Systems:

The System Owner must implement GSA hardening and audit settings which may be obtained from the [IT Security Technical Guides and Standards](#) InSite page.

Additional Contractor System Considerations: None.

3.11 AU-11 Audit Record Retention

Control: The organization retains audit records online for *[archived for a period of not less than 180 days]* to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

GSA Implementation Guidance: Control AU-11 is applicable at all FIPS 199 levels.

Common Control Implementation:

Audit records that have been forwarded to the Enterprise Logging Platform for aggregation and correlation will be stored for at least 180 days. Audit records that have been forwarded to the Enterprise Logging Platform do not simultaneously have to be retained for this amount of time at the log source though it is recommended that they be kept, if possible.

System Specific Expectations for GSA/Internally Operated Systems:

The System Owner is responsible for ensuring that records are either forwarded to the Enterprise Logging Platform as a first preference, or if this is not possible, they must be stored elsewhere in order to meet the 180 day archive requirement.

Additional Contractor System Considerations: None.

3.12 AU-12 Audit Generation

Control: The information system:

- a. Provides audit record generation capability for the auditable events defined in AU-2 a. at *[all components]*;
- b. Allows *[Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians]* to select which auditable events are to be audited by specific components of the information system; and
- c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Control Enhancements:

- (1) Audit Generation | System-Wide / Time-Correlated Audit Trail. The information system compiles audit records from *[all components]* into a system-wide (logical or physical) audit trail that is time correlated to within *[1 minute of UTC]*.
- (3) Audit Generation | Changes by Authorized Individuals. The information system provides the capability for *[Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Owners (e.g., System Program Managers, System Project Managers)]* to change the auditing to be performed on *[all components]* based on *[change management decisions]* within *[minutes]*.

GSA Implementation Guidance: Control AU-12 is applicable at all FIPS 199 levels. Enhancements AU-12(1) and (3) are applicable at the FIPS 199 High level.

Common Control Implementation:

GSA information systems must be capable of generating audit records from the list of auditable events specified in AU-2 for all information system components. These records must be available to authorized personnel for configuration of auditable events, as well as being capable of generating the required audit content as defined in AU-3 of this guide.

For enhancement AU-12(1), GSA FIPS-199 High impact systems audit records must be time correlated to within 1 minute of UTC.

For enhancement AU-12(3), GSA FIPS-199 High impact systems will on a case-by-case basis, after coordination between the GSA OCISO ISO and ISE divisions and system owners and ISSO/ISSM, follow the system's change management process to adjust auditing as necessary.

Additional Contractor System Considerations: None.

4 Summary

Auditing, when properly implemented, helps to accomplish several security-related objectives, including but not limited to individual accountability, detecting security violations and intrusions, identifying flaws in systems and applications, and support in incident reconstruction.

The audit function including the proper setting of audit configurations and the subsequent review and analysis of resultant records is tedious and time consuming work. Accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem is challenging but made easier with automated tools. Such tools can make logs far more useful and reduce the amount of time required for review. Even with automated tools, reviewers must be skilled in information security and know what to look for. They must be effective in spotting unusual activity, understand the normal activity for the systems, and able identify and understand attacks.

Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO, ISP Division for guidance, at ispcompliance@gsa.gov.